Requirement 6.1 to 6.2

Patch Management Policy and Procedures

Overview

One of the most critical initiatives for ensuring the confidentiality, integrity, and availability (CIA) of any organization's information systems environment is that of comprehensive security and patch management procedures. Cyber security threats are posing serious challenges for many I.T. professionals, as attackers and malicious exploits are constantly seeking to penetrate vulnerabilities within one's network architecture. Having critical systems resources operating without the latest security updates poses a serious danger to their safety and security, which in turn can result in these systems being severely compromised. Being proactive and having a well-defined patch management framework – one with documented policies and procedures in place – is what's needed for every organization today, regardless of industry, size, or location.

As for patch management itself, from an information security perspective, it's best defined as the following:

The policies, procedures and related processes undertaken for effectively identifying, acquiring, testing, distributing, installing, and monitoring security patches for all relevant system resources throughout an organization, including, but not limited to, all network devices, operating systems, applications, and other in-scope systems.

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal patch management policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

Purpose

This policy and applicable supporting procedures are designed to provide [company name] with a documented and formalized process for acquiring, testing, distributing, installing, and monitoring security patches. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of [company name]'s system components.

Scope

This policy and supporting procedures encompasses all system components that are owned, operated, maintained, and controlled by [company name] and all other system components, both internally and externally, that interact with these systems.

- Internal system components are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.

- External system components are those owned, operated, maintained, and controlled by any entity other than [company name], but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system components".

- **Note:** While [company name] does not have the ability to actually provision, harden, secure, and deploy another organization's system components, [company name] will follow PCI DSS due-diligence best practices as mandated in Requirement 12 of the Payment Card Industry Data Security Standards by obtaining all relevant information ensuring that such systems are safe and secure.

Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to [company name] information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- **Management Commitment:** Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The [CTO | CIO, or other designated title] is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.

- **Internal Employees and Users:** Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any [company name] system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of [company name] system components, and are to also report such instance immediately to senior authorities.

- **Vendors, Contractors, other Third-Party Entities:** Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

Policy

[Company name] is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

In accordance with best practices for security patch management, the subsequent three (3) security concerns will be highlighted throughout the patch management policy and procedures. They are as follows (NIST, n.d.):

- **Vulnerabilities**: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the cardholder data environment or any other IT resources

- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.
- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the cardholder environment. This includes but is not limited to the following:

- Network devices and all supporting hardware and protocols.
- Operating systems within the development and production environments.
- Applications within the development and production environments.
- Any other mission-critical resources within the cardholder data environment that require patches and security updates for daily operations

Additionally, a Security Patch Management Program (SPMP) is to be implemented, which consists of the following initiatives:

- A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities.
- Comprehensive inventory of all system components directly associated with the cardholder environment.
- Comprehensive inventory of all other IT resources not directly associated with the cardholder environment.
- Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues.
- Procedures for establishing a risk ranking regarding security patch management. This will include but is not limited to (1) the significance of the threat, (2) the existence and overall threat of the exploitation and (3) the risks involved in applying security patch management procedures (its effect on other systems, resources available and resource constraints).
- The creation of a database of remediation activities that needs to be applied.
- Test procedures for testing patches regarding remediation.
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures.
- Procedures for verifying successful implementation of patches and other related security-hardening procedures.
- Installation of applicable critical vendor-supplied security patches within one month of release.
- Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

Security Patch Management Program Employee

This individual(s) will be responsible for coordinating, facilitating and undertaking all necessary activities regarding security patch management policies and procedures. Additionally, this individual(s) will have the necessary information technology and security expertise to successfully execute all steps as required. Specifically, this individual(s) will have a strong working knowledge of vulnerability and patch management, as well as system administration, intrusion detection and firewall management.

Security Patch Management Program Employee

Name	Title	Contact Information
Jason Smith	Senior Network Engineer	smith@company.com
Mike Larson	Backup Network Engineer	Mlarson@company.com
?	?	?
?	?	?
?	?	?

Asset Inventory of All System Components Directly Associated with Cardholder Environment

The following table includes all system components that are directly associated with the cardholder environment. These system components are to be listed by network devices, operating systems, applications and any other system components as needed.

Note: Because many businesses often physically and/or logically isolate their cardholder data environment from other enterprise-wide IT resources, they often list such assets individually – and if that is the case – then you can use the below referenced tables for providing such information. If not, and you have a comprehensive asset inventory list that details ALL of your IT resources, then you can simply remove the below referenced tables and make reference of such a list.]

System Components - Firewalls	Host Name	Physical Location	Owner	Primary Use in Cardholder Data Environment
System Components - Routers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components - Switches	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**

System Components – Load Balancers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components – Web Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components – Application Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components –Database Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**

System Components – Other Servers	Host Name	Physical Location	Owner	Primary Use in Cardholder Data Environment

Inventory of all other IT Resources Not Directly Associated with Cardholder Environment

The following table includes all other IT resources not directly associated with the cardholder environment. These IT resources, however, are still considered critical to the daily operations of [company name] and must be patched accordingly.

Note: If you would like to use this document as your organization's primary patch management policy, then please use the below referenced tables to list all IT resources. If not, and you have a comprehensive asset inventory list that details ALL of your IT resources, then you can simply remove the below referenced tables and make reference of such a list.]

System Components - Firewalls	Host Name	Physical Location	Owner	Primary Use in Cardholder Data Environment
System Components - Routers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components - Switches	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**

System Components – Load Balancers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components – Web Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components – Application Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**
System Components –Database Servers	**Host Name**	**Physical Location**	**Owner**	**Primary Use in Cardholder Data Environment**

System Components – Other Servers	Host Name	Physical Location	Owner	Primary Use in Cardholder Data Environment

Industry-Leading Security Sources and Additional Supporting Resources

Various external security sources and resources are utilized to ensure that [company name] maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available.

Currently, [company name] subscribes to the following types of security sources and resources (NIST, n.d.):

- Vendor websites and email alerts
- Vendor mailing lists, newsletters and additional support channels for patches and security
- Third-party websites and email alerts
- Third-party mailing lists
- Online forums and discussion panels
- Conferences, seminars and trade shows

Listed below are the specific security resources and sources to which [company name] subscribes for patch management, alerts, security and support as applicable:

Online Resources for Patch Management, Alerts, Security and Support, As Applicable

Vendor/Provider and Type of System	Website	Other
CISCO	http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml	Security Advisory Alert Board
IBM AIX	http://www-03.ibm.com/systems/power/software/aix/service.html	AIX support and alert website
Microsoft	http://technet.microsoft.com/en-us/wsus/default.aspx	Windows Server Update Services (WSUS)
Oracle	http://www.oracle.com/technology/deploy/security/alerts.htm	Critical Patch Updates and Security Alerts
Apache	http://www.apache.org/dist/httpd/patches	Official Patches for Apache
?	?	?

?	?	?
?	?	?
?	?	?

Please note: This is just a sample used to illustrate how this section should be completed. For an in-depth listing of all vendors, providers, their products and respective websites, please view Appendix D from the following URL: http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf. Additionally, please add any other vendors that you use.

Risk Ranking for Security Patch Management

A Risk Ranking matrix will be established regarding security patch management. Specifically, system components and other associated IT resources will be given a risk ranking pertaining to the importance of security patch management activities to be undertaken.

In accordance with NIST SP 800-30, [company name] will adhere to the following definitions regarding risks that are related to all system components within the cardholder environment and any other IT resources.

- **High:** The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective.
- **Medium:** The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- **Low:** The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Risk Ranking Table

Critical Security Threats	Response Mechanisms to Initiate	Priority Level 1 (High)	Priority Level 2 (Medium)	Priority Level 3 (Low)
Vendor Patches and security updates defined as "high," "critical" or "urgent" for all system components and other IT resources affected by threat	Please discuss your response mechanisms for these types of security threats.	X		
Vendor Patches and security updates defined as "medium," "moderate" or "important" for all system components and other IT resources affected by threat	Please discuss your response mechanisms for these types of security threats.		X	
Vendor Patches and security updates defined as "low," "non-essential" or "non-urgent" for all system components and other IT resources affected by threat	Please discuss your response mechanisms for these types of security threats.			X
Security alerts from SANS, CERT, NIST, CIS and all other industry-leading associations	Assign risk accordingly based on each individual threat.			

Recommendations from all other industry-leading security sources (online forums, email subscriptions to security forums, etc.) regarding threats	Assign risk accordingly based on each individual threat.			

Additionally, the Security Patch Management Program employee will also be responsible for the following critical activities:

- Being aware of all known threats or vulnerabilities that could significantly impact system components within the cardholder data environment and any other IT resources. This requires consistent oversight and management of all online resources used for security patch management as previously described.
- Having a strong technical and business understanding of all critical systems within the organization's IT infrastructure, as well as knowing which systems are essential for day-to-day operations
- Having response mechanisms and procedures in place to immediately report the scope of the exploitation (systems affected), the impact to the IT infrastructure as a whole and which remediation activities and plan of action initiatives are already available to the management in the event of network exploitation.

Database of Remediation Activities that need to be applied

The database for remediation activities will consist of listing the relevant Uniform Resource Locators (URL) for each patch and specific advice and any other comments deemed critical to the patch itself. Additionally, the Security Patch Management Program employee will be responsible for keeping the database accurate and relevant.

System Components within Cardholder Data Environment and other IT Resources	Uniform Resource Locator (URL) for Patch	Notes/Comments
Oracle	http://www.oracle.com/technology/deploy/security/alerts.html#CriticalPatchUpdates	Online board and listing for Oracle products and their respective patches
Microsoft	http://www.microsoft.com/security/updates/bulletins/default.aspx	Online board and listing for Microsoft products and their respective patches
?	?	?
?	?	?
?	?	?

Test Procedures for Testing Patches Regarding Remediation

Security patch management testing procedures must be observed to ensure the authenticity of the patch or any other security upgrades before they are released to day-to-day operations.

The following testing procedures are to be adhered to (NIST, n.d.):

- An acceptable test environment (non-production systems) will be determined and utilized, if necessary, for each and every patch and security upgrade implemented by the SPMP employee.
- For vendors providing patches, the authenticity of the downloaded patch will need to be verified. This verification process will be determined as needed for patches and security upgrades.
- A virus scan is to be run on all patches before installation.
- Determine *patch dependency* or any other issues that may result in the installation of the patch. Would the installation of the new patch disable another? Are other patches uninstalled when the new patch is installed?

Distribution, Deployment and Implementation of Patches and other Security-Hardening Procedures

All patches and security updates are to be pushed out in a formalized and secure manner, with all critical patches installed within one (1) month of release from a vendor or other approved third party. This includes using the following:

- Enterprise Patch Management software
- Secured email lists sent to authorized personnel
- Secure internal web source for retrieving patches sent out by the SPMP employee

[Listed above are three common examples of deploying patches. Please modify according to your specific environment.]

Verifying Successful Implementation of Patches and other Security-Hardening Procedures

It is the responsibility of the SPMP employee to verify the successful implementation of all patches and security upgrades to [company name]'s IT infrastructure. These activities will consist of, but are not limited to, the following:

- Verifying that the files have been changed as stated in the vendor's documentation to reflect the updates as needed
- Verifying whether the recommended patches and security updates were installed properly by reviewing patch logs

[Listed above are two common examples of verifying the successful implementation of patches and security updates. Please modify according to your specific environment.]

Procedures

[Company name] is to ensure that all applicable users adhere to the following procedures and supporting activities listed below. Additionally, the relevant procedures will be fully enforced by [company name] for ensuring such initiatives are executed in a formal manner and on a consistent basis for all specified systems resources.

1. Undertake all necessary activities for ensuring the aforementioned policies are implemented. This ultimately requires coordination amongst various [company name] personnel, along with utilizing various security tools, vendor documentation, and other supporting materials for ensuring the stated policy mandates are met. [If you have any specific, more detailed "activities" you would like to add in addition to the already mentioned statement above, then please do so here.]

2. Complete the above reference tables and answer all corresponding columns. The tables are to be reviewed on a regular basis, which is at a minimum, twice a year.

3. If changes must be made to system components – such as additional hardening procedures, configuration changes, or any other necessary I.T. changes for ensuring continued compliance with the aforementioned policies – then a ticket/change order is to be opened and submitted in the [name of ticketing system] which effectively details the reason for the change, what actual changes will be made, why, and any other relevant information.

4. [If you have any specific "procedures" you would like to add in addition to the already mentioned policy/procedure statements above, then please use this section to do so. If not, then please delete this section. Keep in mind that not all policy documents require specific stand-alone supporting procedures, as the policy statement itself can be deemed sufficient].

Compliance Cross Reference Matrix

The following Matrix is to be completed for purposes of cross-referencing this specific PCI DSS document with any other mandated regulatory compliance requirements for [company name]. As such, a brief summary describing the contents of this document must be provided, allowing management to effectively cross-reference and align with the below referenced compliance standards, framework and/or regulations, etc.

Document Summary	List of Compliance Standards Frameworks, Regulations	Cross Reference Details	General Notes and Comments
Enter brief summary of the document and its overall purpose.	ISO 27001/27002	*Enter the specific section or reference criteria pertaining to the actual standard, framework, and/or regulations.*	
	ITIL		
	FISMA & NIST SP 800-53 HIPAA and HITECH		
	Gramm Leach Bliley Act (GLBA)		
	Enter additional standards, frameworks, and/or regulations.		

Responsibility for Policy and Procedures Maintenance

[Title of responsible party] is responsible for ensuring that the aforementioned policy initiatives, and if applicable – the relevant procedures – are kept current as needed for purposes of compliance with mandated organizational security requirements set forth and approved by management.

Disclosure

[Company name] reserves the right to change and modify the aforementioned document at any time and to provide notice to all users in a reasonable and acceptable timeframe and format.